Bykovskii's theorem and generalized Larcher's theorem

Dmitry M. Ushanov[1]

Summary

For $a = (a_1, \ldots, a_s) \in \mathbb{Z}^s$ denote by

$$\mathcal{K}(a) = \left\{ \left(\left\{ \frac{a_1 k}{N} \right\}, \cdots, \left\{ \frac{a_s k}{N} \right\} \right) \mid k = 1, 2, \ldots, N \right\}$$

the sequence of *Korobov lattice points* (see [8]).

For any sequence $\Xi = \{\xi_x \in [0,1]^s, \quad x = 0, 1, 2, ..., N-1\}$ denote by

$$D(\Xi) = \sup_{\gamma_1, \ldots \gamma_s \in [0,1]} |\#\{x : 0 \le x < N,\ \xi_x \in [0, \gamma_1) \times \cdots \times [0, \gamma_s)\} - \gamma_1 \cdots \gamma_s N|$$

the *discrepancy* of the sequence.

G. Larcher proved the following theorem (see [3]).

Theorem A. *There is a constant c, such that for every integer N there exists an integer g, with $(g, N) = 1$ and for the sequence $\mathcal{K}(1, g)$ is*

$$D_N(\mathcal{K}(1, g)) < c \frac{N \log N \log\log N}{\phi(N)}.$$

Recently V. Bykovskii proved the following result (see [1], [2]).

Theorem B. *For every integer $s \geqslant 2$ there is a constant c, such that for every integer N there exists an $a = (a_1, \ldots, a_s) \in \mathbb{Z}^s$ with*

$$D_N(\mathcal{K}(a_1, \ldots, a_s)) < c \log^{s-1} N \log\log N.$$

Also, G. Larcher obtained the following result (see [3], Corollary 5). For every $k \in \mathbb{N}$ there is a constant $c(k)$ such that for every $N \in \mathbb{N}$, there exists an $x \in \mathbb{N}$ with $(x, N) = 1$, and

$$\sum b_i < c(k)(\log N \log\log N)^2,$$

where $x^k/N = [b; b_1, b_2, \ldots, b_l]$ is a continued fraction expansion. Therefore (see [6]), one has

$$D(\mathcal{K}(1, x^k)) \ll (\log N \log\log N)^2.$$

N. Moshchevitin and D. Ushanov [5] improved this result of G. Larcher and proved the following theorem.

Theorem C. *Let p be prime, U be a multiplicative subgroup in $\mathbb{Z}_p^*$. For $v \neq 0$ we consider the set $R = v \cdot U$ and let*

$$\#R \geq 10^8 p^{7/8} \log^{5/2} p.$$

[1]research is supported by RFBR grant 12-01-00681

Then there exists an element $a \in R$, $a/p = [b_1, b_2, \cdots, b_l]$, $b_i = b_i(a)$, $l = l(a)$ *with*

$$\sum_{i=1}^{l} b_i \le 500 \log p \log\log p.$$

We would like to note that recently Mei-Chu Chang [9] independently obtained Theorem C.

In present paper we use results of Bykovskii and obtain the following generalization of Larher's theorem.

Theorem 1. *Let*

$$\alpha_m = \frac{2^{m-1}}{2^{m+1} - m - 2}, \quad \beta_m = \frac{2^m}{2^{m+2} - m - 4},$$

$$n_\delta = \max(3, \left\lceil \frac{81}{\delta} + \frac{1}{\ln 2} - 160 \right\rceil).$$

Define $s'(\delta)$ *and* $s''(\delta)$ *as follows*

$$s'(\delta) = \begin{cases} \left\lceil \frac{2m^2(\delta-1)}{4\delta(2^{-m}-1)+1} \right\rceil + 2, & \text{if } \beta_m \leqslant \delta < \alpha_m \\ \left\lceil \frac{2m(\delta-1)(m+1)}{\delta(3\cdot 2^{-m}-4)+1} \right\rceil + 2, & \text{if } \alpha_{m+1} \leqslant \delta < \beta_m, \end{cases}$$

$$s''(\delta) = \left\lfloor \frac{(1-\delta)2^{n_\delta}}{(\delta^{\frac{160+n_\delta}{81}} - 1) \cdot 0.45} \right\rfloor + 3.$$

Set $s_{\min}(\delta) = \min(s'(\delta), s''(\delta))$.

Let $\delta \in (0,\ 1)$ *and integer* $s \geqslant s_{\min}(\delta)$. *Let* $p \geqslant 3$ *be prime,* $G \subset \mathbb{Z}_p^*$ *be a subgroup. If* $\#G \geqslant p^\delta$ *then there exist elements* $a_1, \ldots, a_s \in G$ *with*

$$D_p(\mathcal{K}(a_1, \ldots, a_s)) \ll_{\delta,\ s} \log^{s-1} p \log\log p.$$

Corollary 1. *For small values of* m *in Theorem 1 we get the following. Let* s *be an integer and* δ *be a real such that*

$$s \geqslant \begin{cases} 3, & \delta \in [3/4,\ 1) \\ 4, & \delta \in [2/3,\ 3/4) \\ 5, & \delta \in [14/23,\ 2/3) \\ 6, & \delta \in [4/7,\ 14/23) \\ 7, & \delta \in [6/11,\ 4/7) \\ 8, & \delta \in [10/19,\ 6/11) \\ 9, & \delta \in [22/43,\ 10/19) \\ 10, & \delta \in [1/2,\ 22/43) \\ 11, & \delta \in [17/35, 1/2) \end{cases} \quad s \geqslant \begin{cases} 12, & \delta \in [9/19, 17/35) \\ 13, & \delta \in [19/41, 9/19) \\ 14, & \delta \in [5/11, 19/41) \\ 15, & \delta \in [21/47, 5/11) \\ 16, & \delta \in [11/25, 21/47) \\ 17, & \delta \in [23/53, 11/25) \\ 18, & \delta \in [3/7, 23/53) \\ 19, & \delta \in [25/59, 3/7) \\ 20, & \delta \in [13/31, 25/59). \end{cases}$$

Let $p \geqslant 3$ *be prime,* $G \subset \mathbb{Z}_p^*$ *be a subgroup. If* $\#G \geqslant p^\delta$ *then there exist elements* $a_1, \ldots, a_s \in G$ *with*

$$D_p(\mathcal{K}(a_1, \ldots, a_s)) \ll_{\delta,\ s} \log^{s-1} p \log\log p.$$

The author is grateful to Prof. Igor Shparlinski for pointing out an opportunity of improvement of the main result of the paper.

1. Введение

Пусть $a = (a_1, \dots, a_s)$ — произвольный набор целых чисел, а $N \geqslant 3$ — натуральное число. *Сеткой Коробова* (см. [8]) называется множество

$$\mathcal{K}(a) = \left\{ \left(\left\{ \frac{a_1 k}{N} \right\}, \cdots, \left\{ \frac{a_s k}{N} \right\} \right) \mid k = 1, 2, \dots, N \right\}.$$

Рассмотрим решетку

$$\Gamma_N(a) = \{(m_1, \dots, m_s) \in \mathbb{Z}^s \mid a_1 m_1 + \dots + a_s m_s \equiv 0 \pmod{N}\},$$

несложно проверить, что

$$\mathcal{K}(a) = \Gamma_N^*(a) \cap [0,1)^s,$$

где $\Gamma_N^*(a)$ — двойственная к $\Gamma_N(a)$ решетка.

Для последовательности $\Xi = \{\xi_x \in [0,1]^s, \quad x = 0, 1, 2, ..., N-1\}$ *отклонением* называется следующая величина:

$$D(\Xi) = \sup_{\gamma_1, \dots \gamma_s \in [0,1]} |\#\{x : 0 \leq x < N,\ \xi_x \in [0, \gamma_1) \times \dots \times [0, \gamma_s)\} - \gamma_1 \cdots \gamma_s N|.$$

В [3] Г. Ларчер получил следующий результат.

Теорема A. *Существует постоянная c, такая, что для любого натурального N существует натуральное g, $(g, N) = 1$ и отклонение сетки $\mathcal{K}(1, g)$ оценивается*

$$D_N(\mathcal{K}(1, g)) < c \frac{N \log N \log \log N}{\phi(N)}.$$

Доказательство теоремы элементарно и опирается на аппарат цепных дробей.

Недавно В.А. Быковский получил следующий результат (см. [1], [2]).

Теорема B. *Для любого натурального $s \geqslant 2$ существует постоянная c, такая, что для любого натурального N найдется такой набор $(a_1, \dots, a_s)$, что отклонение сетки $\mathcal{K}(a_1, \dots, a_s)$ оценивается*

$$D_N(\mathcal{K}(a_1, \dots, a_s)) < c \log^{s-1} N \log \log N.$$

Доказательство этой теоремы использует аналитический аппарат.

Ларчер получил также следующий результат для вычетов степени k (см. [3], Следствие 5). Для любого $k \in \mathbb{N}$ существует константа $c(k)$ такая, что для любого $N \in \mathbb{N}$ найдется $x \in \mathbb{N}$, $(x, N) = 1$, $1 \leqslant x < N$, такой что существует x_1, $x \equiv x_1^k \pmod{N}$ и для разложения в цепную дробь $\frac{x}{N} = [0; b_1, \dots, b_l]$ выполнено

$$\sum b_i < c(k)(\log N \log \log N)^2.$$

Отсюда следует (см. Островский [6]) оценка на отклонение двумерной последовательности: для такого x будет верно

$$D(\mathcal{K}(1,x)) \ll (\log N \log\log N)^2.$$

В работе [5] получено усиление теоремы Ларчера на случай когда вместо множества вычетов фиксированной степени при простом N рассматривается произвольная достаточно большая мультипликативная подгруппа группы $\mathbb{Z}_p^*$.

Теорема C. *Пусть p простое, G — мультипликативня подгруппа в $\mathbb{Z}_p^*$. Пусть*

$$\#G \geq 10^8 p^{7/8} \log^{5/2} p.$$

Тогда существует элемент $a \in G$, $a/p = [0; b_1, b_2, \cdots, b_l]$, с

$$D(\mathcal{K}(1,a)) \ll \sum_{i=1}^{l} b_i \leq 500 \log p \log\log p.$$

Пользуясь результатами В.А. Быковского (см. [1], [2]), в настоящей работе мы обобщили результат Ларчера на большие размерности и получили следующую теорему.

Теорема 1. *Обозначим*

$$\alpha_m = \frac{2^{m-1}}{2^{m+1}-m-2}, \quad \beta_m = \frac{2^m}{2^{m+2}-m-4}, \quad n_\delta = \max\left(3, \left\lceil \frac{81}{\delta} + \frac{1}{\ln 2} - 160 \right\rceil\right).$$

Определеним функции $s'(\delta)$ и $s''(\delta)$ следующим образом

$$s'(\delta) = \begin{cases} \left\lceil \frac{2m^2(\delta-1)}{4\delta(2^{-m}-1)+1} \right\rceil + 2, & \text{если } \beta_m \leqslant \delta < \alpha_m, \\ \left\lceil \frac{2m(\delta-1)(m+1)}{\delta(3\cdot 2^{-m}-4)+1} \right\rceil + 2, & \text{если } \alpha_{m+1} \leqslant \delta < \beta_m, \end{cases}$$

$$s''(\delta) = \left\lfloor \frac{(1-\delta)2^{n_\delta}}{(\delta^{\frac{160+n_\delta}{81}} - 1)\cdot 0.45} \right\rfloor + 3.$$

Пусть $s_{\min}(\delta) = \min(s'(\delta), s''(\delta))$.

Если $s \geqslant 3$ и $\delta \in (0,\ 1)$ таковы, что $s \geqslant s_{\min}(\delta)$, то для любого простого $p \geqslant 3$, любой подгруппы G мультипликативной группы $\mathbb{Z}_p^*$, такой, что $\#G \geqslant p^\delta$, найдутся элементы $a_1, \ldots, a_s \in G$, для которых верно

$$D_p(\mathcal{K}(a_1, \ldots, a_s)) \ll_{\delta,\ s} \log^{s-1} p \log\log p.$$

2. Основые идеи доказательства

Всюду далее мы будем использовать следующие обозначения. Пусть G — подгруппа мультипликативной группы $\mathbb{Z}_p^*$ чисел по модулю p. Обозначим через $A(P_1, ..., P_s)$ число решений сравнения

$$a_1 m_1 + \cdots + a_s m_s \equiv 0 \pmod p$$

в целых $a_1, \dots, a_s \in G$ и целых $m_1, \dots, m_s$, таких, что

$$1 \leqslant m_1 \leqslant P_1, \dots, 1 \leqslant m_s \leqslant P_s.$$

Лемма 1. *Пусть параметры s и δ выбраны так, как в теореме 1. Тогда*

$$A(P_1, \dots, P_s) \ll \frac{\# G^s}{p} P_1 \cdots P_s.$$

Доказательство. Обозначим $e_p(t) = \exp(2\pi i t/p)$,

$$S(t, G) = \sum_{g \in G} e_p(tg),$$

$$S(G) = \max_{t \neq 0} |S(t, G)|.$$

Сначала рассмотрим случай, когда $s \geqslant s'(\delta)$.

Заметим, что количество решений сравнения равно

$$A(P_1, \dots, P_s) = \frac{1}{p} \sum_{1 \leqslant m_i \leqslant P_i} \sum_{a_i \in G} \sum_{n=1}^{p} e_p(n(a_1 m_1 + \dots + a_s m_s)).$$

Воспользовавшись неравенством Коши-Буняковского, получим

$$A(P_1, \dots, P_s) \leqslant \frac{1}{p} \sum_{m} S^{s-2}(G) \cdot p \# G. \tag{1}$$

Для оценки $S(G)$ сверху мы воспользуемся результатом Конягина (см. [4]). А именно, в обозначениях формулировки теоремы 1

1. если существует $m \in \mathbb{N}$, что $\beta_m \leqslant \delta < \alpha_m$, то

$$S(G) \ll_m \# G^{1 - \frac{2}{m^2} + \frac{1}{2^{m-1} m^2}} p^{\frac{1}{2m^2}},$$

2. если же существует $m \in \mathbb{N}$, что $\alpha_{m+1} \leqslant \delta < \beta_m$, то

$$S(G) \ll_m \# G^{1 - \frac{2}{m(m+1)} + \frac{3}{2^{m+1} m(m+1)}} p^{\frac{1}{2m(m+1)}}.$$

Подставляя оценки на $S(G)$ в оценку (1) для $A(P_1, \dots, P_s)$, мы получим

$$A(P_1, \dots, P_s) \leqslant \frac{\# G^s}{p} P_1 \cdots P_s.$$

В случае $s \geqslant s''(\delta)$ мы рассуждаем так же, разница заключается в другой оценке $S(G)$.

Мы используем следующий результат Гараева (см. [7], теорема 4.1). Если $3 \leqslant n \leqslant 1.44 \log\log p$ — натуральное число, $c > 0$ — произвольная постоянная, $X_1, \dots, X_n$ — подмножества Z_p^*, удовлетворяющие условию

$$\# X_1 \cdot \# X_2 \cdot (\# X_3 \cdots \# X_n)^{1/81} > p^{1+c},$$

то имеет место оценка

$$\left| \sum_{x_1 \in X_1} \cdots \sum_{x_n \in X_n} e_p(x_1 \cdots x_n) \right| \ll \#X_1 \cdots \#X_n p^{\frac{-0.45c}{2^n}}.$$

Взяв $X_1 = tG$, $X_2 = G, \ldots, X_n = G$, и подобрав подходящим образом параметры c и n, мы получим лемму. $\square$

3. Схема доказательства теоремы 1

Выберем параметр $Q = \frac{p}{2\log^{s+1} p}$. Пусть $a = (a_1, \ldots, a_s)$. Для целочисленного вектора $m = (m_1, \ldots, m_s)$ определим

$$H(m) = \max(1, |m_1|) \cdots \max(1, |m_s|).$$

Определим функцию

$$q(a) = \min\{H(m) \mid a_1 m_1 + \cdots + a_s m_s \equiv 0 \pmod{p}\}.$$

Определим множества Ω_1 и Ω следующим образом:

$$\Omega_1 = \{a \in G^s \mid q(a) \leqslant Q\},$$

$$\Omega = \{a \in G^s \mid q(a) > Q\}.$$

Очевидно, что $\#(\Omega_1 \cup \Omega) = \#G^s$. С помощью леммы 1 мы показываем, что $\#\Omega_1 \leqslant \#G^s/2$, следовательно $\#\Omega > \#G^s/2$.

Ненулевой узел γ решетки Γ называется *относительным минимумом*, если не найдется другого ненулевого узла γ' из Γ, для которого

$$|\gamma_1'| \leqslant |\gamma_1|, \ \ldots, \ |\gamma_s'| \leqslant |\gamma_s|.$$

Обозначим через $\mathfrak{M}(\Gamma)$ множество всех относительных минимумов решетки Γ.

Далее мы воспользуемся следующим результатом В.А. Быковского (см. [2]): для любой сетки Коробова верно неравенство

$$D_N(\mathcal{K}(a)) \ll N \sum_{m \in \mathfrak{M}(\Gamma_N(a))} \frac{1}{H(m)}.$$

Таким образом, усредняя по множеству $\#\Omega$, мы получим

$$\min_{a \in G^s} D(\mathcal{K}(a)) \ll \frac{p}{\#\Omega} \sum_{a \in G^s} \sum_{Q \leqslant H(m) \leqslant p} \frac{\delta_p(a_1 m_1 + \cdots + a_s m_s)}{H(m)}.$$

Оценивая последнюю сумму, мы получаем теорему.

Список литературы

[1] V.A. Bykovskii, *The discrepancy of the Korobov lattice points.* Program and Abstract Book, p.10-11. 27th Journees Arithmetiques conference.

[2] В.А. Быковский, *Отклонение сеток Коробова*, Известия РАН, (принято в печать)

[3] Gerhard Larcher, *On the Distribution of Sequences Connected with Good Lattice Points.* Monatshefte fur Mathematic 101 (1986), pp. 135 - 150.

[4] С.В. Конягин *Оценки тригонометрических сумм по подгруппам и сумм Гаусса*, IV Межденародная конференция "Современные проблемы теории чисел и ее приложения 2002, Часть 3

[5] Nikolay G. Moshchevitin, Dmitrii M. Ushanov *On Larcher's theorem concerning good lattice points and multiplicative subgroups modulo p*, Uniform Distribution Theory 5 (2010), no.1, 45-52

[6] Ostrowski A., *Bemerkungen zur Theorie der Diophantischen Approximationen*, I, II, III. – Abh. Math. Sem. Hamburg, 1922, 1, S. 77-98, S. 250-251

[7] М. З. Гараев, *Суммы и произведения множеств и оценки рациональных тригонометрических сумм в полях простого порядка*, УМН, 65:4(394) (2010), 5Ц66

[8] Н.М. Коробов, *О некоторых вопросах теории диофантовых приближений*, Успехи математических наук, т. 22, вып. 3(135), (1967), с. 83-118.

[9] M.-C. Chang, *Partial quotients and equidistribution*, Comptes Rendus Mathematique. 349:13-14 (2011), 713 - 718.

Dmitry M. Ushanov
E-mail: ushanov.dmitry@gmail.com